

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-008589

(43)Date of publication of application : 10.01.2003

(51)Int.Cl.

H04L 12/28
H04L 29/08
H04N 1/00
H04Q 7/38

(21)Application number : 2001-192179

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 26.06.2001

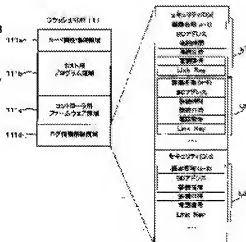
(72)Inventor : KOBAYASHI KOICHI

(54) COMMUNICATION APPARATUS, COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication apparatus having the same communication card that can simplify a radio communication link establishing job when connected to an external device having been connected before even if a host device mounted with the communication card differs.

SOLUTION: A log information storage area 111d is provided to a flash ROM 111 of an SD card 13 and stores log information when the SD card 13 is mounted to a host device such as a personal computer 1 and performs radio communication with an external device. Then when another host device such as a PDA 21 performs radio communication with the same external device, the host device downloads the log information from the log information storage area 111d so as to simplify radio link setup.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51) Int.Cl. ⁷	識別記号	F I	キーワード [*] (参考)
H 0 4 L 12/28	3 0 0	H 0 4 L 12/28	3 0 0 Z 5 C 0 6 2
29/08		H 0 4 N 1/00	1 0 7 A 5 K 0 3 3
H 0 4 N 1/00	1 0 7	H 0 4 L 13/00	3 0 7 A 5 K 0 3 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R 5 K 0 6 7

審査請求 未請求 請求項の数19 ○L (全 20 頁)

(21) 出願番号 特願2001-192179(P2001-192179)

(22) 出願日 平成13年6月26日(2001.6.26)

(71) 出願人 00003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 小林 浩一

東京都青葉市末広町2丁目9番地 株式会社

社東芝青葉工場内

(74) 代理人 100083161

弁理士 外川 英明

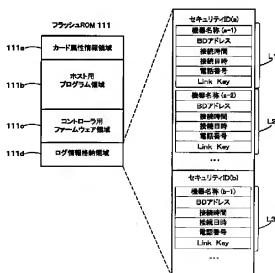
最終頁に続く

(54) 【発明の名称】 通信装置、通信システム及び通信方法

(57) 【要約】

【課題】通信カードが同一であって、過去に接続したことのある外部機器と接続する場合には、通信カードが装着されるホスト装置が異なっても無線通信リンク確立作業を簡略化することのできる通信装置を提供することにある。

【解決手段】SDカード13のフラッシュROM111内にログ情報格納領域111dを設け、このSDカード13がパソコン1等ホスト装置に装着されて外部機器と無線通信を行った際のログ情報をこのログ情報格納領域111dに保存する。次にPDA21等他のホスト装置から上記同一の外部機器と無線通信する際に上記ログ情報格納領域111dからログ情報をダウンロードして利用し、無線リンク確立を簡略化する。



【特許請求の範囲】

【請求項 1】 複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第 1 の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第 1 の手順より簡略な第 2 の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする通信装置。

【請求項 2】 複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、上記通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第 1 の手順で、上記記憶手段に通信履歴情報が記憶されて且つ上記解除手段でアクセス制限が解除された場合は上記第 1 の手順より簡略な第 2 の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする通信装置。

【請求項 3】 複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第 1 の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第 1 の手順より簡略な第 2 の手順で、無線通信リンクを確立する確立手段と、

この確立手段による無線通信リンク確立に先立ち、周囲に存在する無線通信可能な機器を探索し、この探索結果情報と上記通信履歴情報とをホスト装置に出力する出力手段と、を具備することを特徴とする通信装置。

【請求項 4】 複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介し、外部装置との間で無線通信を行う通信手段と、この通信手段と外部装置との間で鍵情報がない場合の第 1 の手順、及上記鍵情報がある場合の上記第 1 の手順より簡易な第 2 の手順のいずれかで無線リンクを確立する確立手段と、

この確立手段が上記第 1 の手順で無線リンクを確立する

ことに伴い上記鍵情報を生成する生成手段と、この生成手段にて生成された上記鍵情報を記憶する記憶手段と、

上記確立手段が無線リンクを確立する際、外部装置が共通であれば、ホスト装置が変更されることに問わず、上記記憶手段に記憶された鍵情報を用いて上記第 2 の手順で行うよう確立手段を制御する制御手段と、を具備することを特徴とする通信装置。

【請求項 5】 複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介し、外部装置との間で無線通信を行う通信手段と、この通信手段と外部装置との間で鍵情報がない場合の第 1 の手順、及上記鍵情報がある場合の上記第 1 の手順より簡易な第 2 の手順のいずれかで無線リンクを確立する確立手段と、

この確立手段が上記第 1 の手順で無線リンクを確立することに伴い上記鍵情報を生成する生成手段と、

この生成手段にて生成された上記鍵情報を記憶する記憶手段と、

この記憶手段に記憶された上記鍵情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、この解除手段でアクセス制限が解除された場合に限り、上記確立手段が無線リンクを確立する際、外部装置が共通であれば、ホスト装置が変更されることに問わず上記記憶手段に記憶された上記鍵情報を用いて上記第 2 の手順で行うよう確立手段を制御する制御手段と、を具備することを特徴とする通信装置。

【請求項 6】 複数のホスト装置に対し着脱可能であり、装着されたホスト装置と通信する第 1 の通信手段と、

ホスト装置に装着された状態で、上記第 1 の通信手段を介して受領したデータを外部装置との間で無線により通信する第 2 の通信手段と、

この第 2 の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記第 2 の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第 1 の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第 1 の手順より簡略な第 2 の手順で、無線通信リンクを確立する確立手段と、を具備し、外部機器が共通であれば、ホスト装置が替わっても上記第 2 の手順による無線通信リンク確立を実行することを特徴とする通信装置。

【請求項 7】 ホスト装置が使用する無線通信用のドライバソフトウェアを記憶する第 2 の記憶手段を有し、ホスト装置に装着された状態で上記ドライバソフトウェアをホスト装置に出力することを特徴とする請求項 6 記載の通信装置。

【請求項 8】 上記記憶手段に通信履歴情報を記憶する

際、同一の外部機器に対する通信履歴情報が記憶されている場合は、この既に記憶されている通信履歴情報を新たな通信履歴情報に置き替えることを特徴とする請求項6記載の通信装置。

【請求項9】 上記記憶手段に通信履歴情報を記憶する際、記憶容量が不足している場合には、接続日時之最も古い通信履歴情報を新たな通信履歴情報に置き替えることを特徴とする請求項6記載の通信装置。

【請求項10】 複数のホスト装置に対し着脱可能であり、装着されたホスト装置と通信する第1の通信手段と、

ホスト装置に装着された状態で、上記第1の通信手段を介して受領したデータを外部装置との間で無線により通信する第2の通信手段と、

この第2の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記第2の通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されてい

かつ上記解除手段でアクセス制限が解除された場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、を具備し、外部機器が共通であれば、ホスト装置が替わっても上記第2の手順による無線通信リンク確立を実行することを特徴とする通信装置。

【請求項11】 上記制限手段は、上記通信履歴情報に対しセキュリティIDを設定する設定手段を有し、上記解除手段は、セキュリティIDを入力する入力手段と、この入力手段で入力されたセキュリティIDが上記設定手段にて設定されたセキュリティIDと一致することを比較する比較手段と、を有することを特徴とする請求項10記載の通信装置。

【請求項12】 上記設定手段は複数のセキュリティIDを設定し、上記解除手段はこれらのセキュリティID毎に解除することを特徴とする請求項11記載の通信装置。

【請求項13】 複数のホスト装置に対し着脱可能であり、装着されたホスト装置と通信する第1の通信手段と、

ホスト装置に装着された状態で、上記第1の通信手段を介して受領したデータを外部装置との間で無線により通信する第2の通信手段と、

この第2の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記第2の通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されていかつ上記解除手段でアクセス制限が解除された場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、この確立手段による無線通信リンク確立に先立ち、周囲に存在する無線通信可能な機器を探索し、この探索結果情報と上記通信履歴情報とをホスト装置に出力する出力手段と、を具備することを特徴とする通信装置。

【請求項14】 通信装置とこの通信装置を介して外部機器とデータ通信を行うホスト装置とからなる通信システムにおいて、

上記通信装置は、

上記ホスト装置との間でデータ通信を行う第1の通信手段と、

この第1の通信手段を介して送受されるデータを外部装置との間で無線通信する第2の通信手段と、

この第2の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記第2の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、を有し、

上記ホスト装置は、上記第1の通信手段とデータ通信する通信手段を有することを特徴とする通信システム。

【請求項15】 通信装置とこの通信装置を介して外部機器とデータ通信を行うホスト装置とからなる通信システムにおいて、

上記通信装置は、

上記ホスト装置との間でデータ通信を行う第1の通信手段と、

この第1の通信手段を介して送受されるデータを外部装置との間で無線通信する第2の通信手段と、

この第2の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、

この制限手段のアクセス制限を解除する解除手段と、

上記第2の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されていてかつ上記解除手段でアクセス制限が解除されている場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、を有し、

上記ホスト装置は、

上記第1の通信手段とデータ通信する通信手段と、

上記制限手段がアクセス制限に使用する情報、及び上記解除手段がアクセス制限の解除に使用する情報を入力する入力手段と、を有することを特徴とする通信システム。

【請求項16】 通信装置とこの通信装置を介して外部機器とデータ通信を行うホスト装置とからなる通信システムにおいて、

上記通信装置は、

上記ホスト装置との間でデータ通信を行う第1の通信手段と、

この第1の通信手段を介して送受されるデータを外部装置との間で無線通信する第2の通信手段と、

この第2の通信手段が通信した外部機器との通信履歴情報を記憶する記憶手段と、

上記第2の通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、

この確立手段による無線通信リンク確立に先立ち、周囲に存在する無線通信可能な機器を探索し、この探索結果情報と上記通信履歴情報とを上記第1の通信手段を介して上記ホスト装置へ出力する出力手段と、を有し、上記ホスト装置は、

上記第1の通信手段とデータ通信する通信手段と、上記出力手段により出力された上記探索結果情報と上記通信履歴情報とを表示する表示手段と、を有することを特徴とする通信システム。

【請求項17】 複数のホスト装置と選択的に通信し、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信方法において、無線通信を行った外部機器との通信履歴情報を記憶し、外部機器と無線通信リンクを確立する際、当該外部機器に対する上記通信履歴情報が記憶されているかを判断し、

上記通信履歴情報が記憶されていない場合は第1の手順で、上記通信履歴情報が記憶されている場合は上記第1の手順より簡略な第2の手順で無線通信リンクを確立することを特徴とする通信方法。

【請求項18】 複数のホスト装置と選択的に通信し、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信方法において、無線通信を行った外部機器との通信履歴情報を記憶し、記憶した上記通信履歴情報へのアクセスを特定の解除情報がない限り禁止し、

外部機器と無線通信リンクを確立する際、アクセス可能で且つ当該外部機器に対する上記通信履歴情報が記憶されているかを判断し、

上記通信履歴情報が記憶されていない場合は第1の手順

で、上記通信履歴情報が記憶されている場合は上記第1の手順より簡略な第2の手順で無線通信リンクを確立することを特徴とする通信方法。

【請求項19】 複数のホスト装置と選択的に通信し、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信方法において、無線通信を行った外部機器との通信履歴情報を記憶し、外部機器と無線通信リンクを確立する際、周囲に存在する無線通信可能な機器を探索し、

探索した結果情報と上記記憶した通信履歴情報とをホスト装置に出力し、

ホスト装置からの外部機器を特定する情報を受け、上記通信履歴情報が記憶されていない外部機器の場合は第1の手順で、上記通信履歴情報が記憶されている外部機器の場合は上記第1の手順より簡略な第2の手順で無線通信リンクを確立することを特徴とする通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、Bluetooth方式等の通信機能を有し、ホスト装置としての各種電子機器に着脱可能に構成された通信装置、この通信装置とホスト装置とからなる通信システム、及び通信方法に関する。

【0002】

【従来の技術】近年、パーソナルコンピュータ（以下、パソコンと称する）、携帯型個人情報端末（以下、PDAと称する）、及び携帯電話等の様々な電子機器が普及している。そして、これら電子機器間のデータ授受をサポートすることを目的として、Bluetooth方式の無線通信機能を持つPCMCIA規格に準拠したカード（以下、PCカードと称する）やSDMMIセキュリティ準拠のSDカードも市場に出はじめている。これらPCカードやSDカードによって上記電子機器はホスト装置であり、ホスト装置に装着された状態でホスト装置と外部機器間でデータを仲介するよう無線通信する。Bluetooth方式の場合、通信データに対するセキュリティ向上を目的として、機器間で無線通信リンクを確立する際には相互認証を行うことにより、不特定の者がデータ取得することを防止している。但し、両機器間で1度の無線通信リンクを確立すると、2度目以降無線通信リンク確立作業を簡略化できるため、最初の無線通信時のログ情報やホスト装置の電子機器に記憶し、活用している。

【0003】しかしながら最近の電子機器の普及率はめざましく、1人の使用者が複数の機器を所有することが珍しくなくなっている。例えば使用者がパソコン、PDA、及びSDカードを所有している場合、パソコンのデータを外部機器に送信する場合にはSDカードをパソコンに装着し、PDAのデータを外部機器に送信する場合にはSDカードをこのPDAに差込めて使用することに

なる。しかしながら、無線通信リンク確立に必要となるログ情報がホスト装置であるパソコン及びPDAのそれぞれに記憶されてしまうため、外部機器が同一のものであってもホスト装置がパソコンからPDAに替わった場合、2度目の無線通信リンク設定であるにも拘わらず、無線通信リンク確立作業を簡略化できない。

【0004】従来より、無線通信機能を有する着脱可能なカードの側に、送受信履歴を記憶する技術は特開2001-77878で知られている。しかしながら、この送受信履歴は認証が伴う無線通信リンクの確立手順を簡略化するものではなく、例えこのようなカードを用いたとしても、同じ認証作業を繰り返すことになることになる。

【0005】

【発明が解決しようとする課題】従来、通信カードは無線接続時の認証に必要なログ情報を記憶せず、パソコン及びPDA等の電子機器側、つまりホスト装置側に記憶する構成となっていた。このため、使用者が、特定の通信カードを用いて、異なるホスト装置と同一の外部機器とを無線接続する場合、その都度認証を含む無線通信リンク確立作業を行わなければならないという問題があった。

【0006】そこで本発明は、通信カードが同一であって、過去に接続したことの外部機器と接続する場合、通信カードが装着されるホスト装置が異なったとしても無線通信リンク確立作業を簡略化することのできる通信装置、通信システム、及び通信方法を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、この発明に係る通信装置は、複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部装置との通信履歴情報を記憶する記憶手段と、上記通信手段と外部装置との間で無線通信リンクを確立するものであって、上記記憶手段に通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されている場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、を具備することとを特徴とする。

【0008】さらにこの発明に係わる通信装置は、複数のホスト装置と選択的に通信可能であり、且つホスト装置と外部装置との間のデータ通信を仲介して外部装置との間で無線通信を行う通信手段と、この通信手段が通信した外部装置との通信履歴情報を記憶する記憶手段と、この記憶手段に記憶された上記通信履歴情報へのアクセスを制限する制限手段と、この制限手段のアクセス制限を解除する解除手段と、上記通信手段と外部装置との間の無線リンクを確立するものであって、上記記憶手段に

通信履歴情報が記憶されていない場合は第1の手順で、上記記憶手段に通信履歴情報が記憶されて且つ上記解除手段でアクセス制限が解除された場合は上記第1の手順より簡略な第2の手順で、無線通信リンクを確立する確立手段と、を具備することを特徴とする。

【0009】上記のように構成された通信装置によれば、過去に接続したことの外部機器と接続する場合、無線通信リンク確立作業を簡略化することができ

る。

【0010】さらに、通信履歴情報に対するアクセスに制限を加えることができるので、通信装置の紛失や盗難により第三者に渡ってしまったとしても、通信履歴情報を不正にダウンロードされることを防止できる。

【0011】

【発明の実施の形態】以下図面を参照して本発明の実施の形態について説明する。図1は本実施形態に係わる通信装置、及び外部機器からなる無線通信ネットワークの概略を示す図である。

【0012】パソコン1は、上面部にキーボード3を備えた本体5と、前面部に表示用LCD7を備えた蓋部9とが、ヒンジ部11を介して開閉可能なノートタイプである。本体5の側面には、SDカード13を装着するための、SDカードインターフェース仕様に準拠したSDカードスロット15が形成されている。SDカード13はBluetooth方式の無線通信機能を有している。

【0013】上記パソコン1とは独立した機器であるPDA21は、LCDと透明なタッチセンサパネルとを重ねたタブレット3を有しており、使用者による入力ペン25の操作に応じてモード設定やデータ入力等が行われる。PDA21の側面にも、SDカード13を装着するための、SDカードスロット27が形成されている。

【0014】これらパソコン1とPDA21は、特定の使用者が所有する機器であり、これに対してパソコン31、FAX33、プリンタ35、PDA37、及びパソコン39は外部機器となる。各外部機器には、SDカード13が装着時されたパソコン1及びPDA21とBluetooth方式の無線通信を行うため、それぞれ無線通信部31a、33a、35a、37a、及び39aを備えている。

【0015】例えば、パソコン1で作成したデータをFAX送信したい場合、SDカード13と無線通信部33aとの間でデータの無線送受信を行い、FAX33は受信したデータを公衆回線を介して所定の相手へFAX送信する。またパソコン1のデータを印刷したい場合、SDカード13と無線通信部35aとの間でデータの無線送受信を行い、プリンタ35は受信したデータを紙に印刷する。もし、その後PDA21のデータを印刷したく

なった場合、SDカード13をPDA21に装着し、SDカード13と無線通信部35aとの間でデータの無線送受信を行い、プリンタ35は受信したデータを紙に印刷する。本実施形態によれば、このプリンタ35のように外部機器が同一で、且つ同一のSDカード13を使用してパソコン1とPDA21のように異なる機器と無線通信する場合、無線リンク確立前の認証作業を簡略化することになる。

【0016】続いて、本実施形態におけるパソコン1、PDA21、及びSDカード13の具体的な構成を詳細に説明する。

【0017】パソコン1の本体5は、図2に示すようにパソコン1の動作を制御するCPU41を有している。CPU41は、CPUバス43及びホスト-PCIブリッジ45を介して主メモリ47、VRAMを含むグラフィックスコントローラ9、及びPCIバス51に接続している。CPU41は主メモリ47にロードされるオペレーティングシステム、アプリケーションプログラム、及びBIOSを実行する。ホスト-PCIブリッジ45は、CPUバス43とPCIバス51とを接続するためのバスブリッジであり、さらに主メモリ47を制御するメモリコントロール機能、及びグラフィックスコントローラ49との間のデータ転送を行なう機能も備えている。グラフィックスコントローラ49は、LCDパネル7に接続している。LCDパネル7は、グラフィックスコントローラ49内に設けられた図示しないVRAMに記憶された情報のパターンデータに基づいて無線通信設定の際のメッセージやアイコン、その他各種情報を表示する。

【0018】PCIバス51には、SDカードコネクタ52を介してSDカード13とデータ送受信を行なうSDホストコントローラ53、PCカードコネクタ54を介してPCカードとのデータ送受信を行うPCホストコントローラ55、PCI-ISAブリッジ47、及びUSB他外部インタフェース59が接続している。SDカードコネクタ52は、SDカードスロット15内に配置され、SDカード13の装着有無を検出するスイッチ61を備えている。PCカードコネクタ54は、本体5内に形成されたPCカードスロット63内に設けられている。PCI-ISAブリッジ47は、PCIバス51をISAバス65に接続するためのバスブリッジであり、さらに内蔵型のHDD67が接続されている。HDD67は、オペレーティングシステム、SDカード13を使用して無線通信を行うためのドライバソフト等のアプリケーションソフトウェア、及びデータを格納しており、各ソフトウェア及びデータはソフトウェア実行時に主メモリ47へロードされる。上記ドライバソフトは、SDカード13が初めて装着された際に自動ダウンロードして保存したものである。またHDD67は、SDカード13を介して外部機器と無線通信した際のログ情報等必要なデータを記憶格納する。

【0019】ISAバス65には、キーボード3、BIOS-ROM69、及びEmbedded Controller（以下、ECと称する）71が接続されている。キーボード3はアキュポイント等のポインティングデバイスを備えている。さらにEC71には、電源コントローラ73、パワースイッチ75、各種報知用LED77が接続している。BIOS-ROM69は、パソコン1内の各ハードウェアを制御するためのルーチンを体系化したプログラムであるBIOSを格納している。EC71は、電源コントローラ73と協働してパソコン1全体及び各デバイスの電源オン/オフを制御する電源シーケンス制御機能を提供する。

【0020】次にPDA21の具体的な構成を図3を用いて説明する。

【0021】PDA21もパソコン1と同様にCPU81を有している。このCPU81には内部バス83を介してフラッシュROM85、RAM87、VRAM89、LCD91、タッチセンサパネル93、SDカードコネクタ94を介してSDカード13とデータ送受信を行うSDホストコントローラ95、及びEC97が接続している。SDカードコネクタ94は、SDカードスロット27内に配置され、SDカード13の装着有無を検出するスイッチ99を備えている。EC97には、電源コントローラ101、パワースイッチ103、及び各種報知用のLED105が接続している。

【0022】CPU81はPDA21全体の制御を司るもので、フラッシュROM85に記憶されたソフトウェアを実行することにより各種機能を実行する。フラッシュROM85は、CPU81を動作させるためのプログラム及び各種初期データを格納するための読み専用メモリ装置であり、SDカード13の最初の装着時に自動ダウンロードされる無線通信用のドライバソフトを記憶して、SDカード13を介して無線通信した際のログ情報等必要なデータの記憶も行う。RAM87は、CPU81による読み書き可能なメモリ装置であり、各種データを一時的に記憶させる作業領域として使用する。LCD91は、VRAM89に記憶された情報のパターンデータに基づいて無線通信設定の際のメッセージやアイコン、その他各種情報を表示する。このLCD91には、タッチセンサパネル93が重畳して設けられてタブレット23を構成し、入力ペン25の接触によりデータ入力を行なう。EC97は、電源コントローラ101と協働してPDA21全体及び各デバイスの電源オン/オフを制御する電源シーケンス制御機能を提供する。

【0023】続いてSDカード13の具体的な構成を図4を用いて説明する。

【0024】SDカード13には、Bluetooth方式無線通信用の構成としてコントローラ101、このコントローラ101の動作クロックを生成する水晶発振器103、外部機器との間で電波送受信するためのアン

テナ105、及び無線通信中であることを報知するLED107が実装されている。コントローラ101はバス109を介してフラッシュROM111及びSD/IOコントローラ113に接続している。さらにSD/IOコントローラ113は、I/Oバス115を介してSDコネクタ117に接続し、水晶発信器119から供給される動作クロックにより動作する。SDコネクタ117は、SDカード13表面に設けられた9つの信号ピンを含んでおり、パソコン1のSDカードコネクタ52やPDA21のSDカードコネクタ94に物理的に接続し、データ送受信を行う。またホスト装置からこのSDカード13へ、SDコネクタ117を介して電力が供給される。

【0025】コントローラ101は、ISMバンドと称される2.4GHz帯の産業用バンドの無線電波によって他の1以上の無線通信装置との間で無線データ通信を行うことが可能な無線通信モジュールであり、周波数ホッピングを用いたスペクトラム拡散方式で近距離無線データ通信を実行する。このコントローラ101は、1チップにて実現されており、大きく高周波回路部（以下、RF部と称する）121とベースバンドコントローラ123とに分かれる。RF部121は高周波信号の送受信を扱うRFトランシーバ回路やRFアンプ及びその制御部分を含んでいる。ベースバンドコントローラ123は、リンク制御やホッピングパターン制御等を初めとするベースバンド処理を行うための機能モジュールである。そして、ベースバンドコントローラ123は、ファームウェアに従ってベースバンド処理を実行するMPU125、作業領域としてのRAM127、無線リンク確立のための制御を行うリンクコントローラ129、及びフラッシュROM111から読み出しSD/IOコントローラ113へ送受するデータを一時的に保存するレジスタ131を備えている。

【0026】アンテナ105は、セラミック製のチップアンテナにより構成されており、RF部121と電気的に接続し2.4GHz帯の無線信号の放射・誘導を行う。

【0027】フラッシュROM111は、図5に示すように、カード属性情報領域111a、ホスト用プログラム領域111b、コントローラ用ファームウェア領域111c、及びログ情報格納領域111dの4つの記憶領域を有している。カード属性情報領域111aでは、SDカード13の属性情報として、例えば無線通信機能を有するI/Oカードであること等の情報を格納している。ホスト用プログラム領域111bには、SDカード13を装着した際に、ホスト機器が使用するドライバソフトウェア（以下、ホスト用ドライバと称する）を格納しており、ホスト装置がホスト用ドライバを保持していない場合には、自動的にアップロードされる。この機能はホスト機器が予めホスト用ドライバを持つ必要がなく、ま

たPDA21やデジタルカメラのようなソフトウェアのインストールが困難なホスト機器にとっては非常に有用なものとなる。コントローラ用ファームウェア領域111cには、コントローラ101が使用するファームウェアを格納しており、無線通信実行に際してRAM127に読みこまれ、MPU125によって実行される。

【0028】ログ情報格納領域111dは、外部機器との無線通信の履歴及びその無線通信により生じたログ情報を格納する。この領域はさらに、セキュリティID毎に区切られており、複数の使用者が個別にセキュリティIDを設定して、各々個別にログ情報を記憶させ活用できる構成となっている。例えばセキュリティID(a)の領域には、ログ情報L1、L2、…が格納されており、セキュリティID(b)の領域にはログ情報L3、…が格納されている。各ログ情報は、無線リンク確立した相手機器の機器名称、デバイスアドレス（以下、BDアドレスと称する）、接続時間、接続日時、電話番号、認証に必要なリンクKeyを含んでいる。後述するとおり、次回以降の接続時及びその認証作業の際に特に重要になるのが機器名称とリンクKeyである。

【0029】SD/IOコントローラ113はパソコン1やPDA21といったホスト機器との間のインターフェースを行うためのカードインターフェースであり、1チップLSIにて実現されている。SD/IOコントローラ113は、制御レジスタ113a、出力データレジスタ113b、及び入力データレジスタ113cを有しており、ホスト機器とコントローラ101との通信は、このSD/IOコントローラ113を介して行われる。例えば、データをホスト機器に送出する場合には、MPU125が制御レジスタ113aの特定ビットのデータを変更すると共に、レジスタ131のデータを出力データレジスタ113bに書き込む。ホスト機器側のCPUは、所定の間隔でこの制御レジスタ113aにアクセスし、上記特定ビットの状態から出力データレジスタ113bにデータがあることを検出すると、出力データレジスタ113bからデータを取り出すというように動作する。

【0030】上述した構成のパソコン1とSDカード13とを用いて外部機器であるプリンタ35と無線通信を行うための一連の動作を説明する。尚、PDA21にSDカード13を装着して外部機器と無線通信する場合も、一連の動作としては基本的に同じである。

【0031】本実施形態の無線通信動作の全体流れは、図6に示す通りである。

【0032】パソコン1のSDカードスロット15にSDカード13が装着されると、スイッチ61がこれを検知し、ホストコントローラ53からPCバス15を経由してCPU41へSDカード挿入されたことを通知する（ステップS1）。CPU41はこの通知を受けると、SDカード13のフラッシュROM111のホスト

用プログラム領域111bに格納されたホスト機器であるパソコン1用のホスト用ドライバがHDD67に既にダウンロードされているかを調べる(ステップS2)。ホスト用ドライバがダウンロード済であれば、CPU41はキーボード3からホスト用ドライバの起動要求、つまり無線通信実行要求が与えられるのを待つ(ステップS3)。上記ステップS3にてホスト用ドライバのダウンロードが行われていない場合には、SDカード13からホスト用ドライバをダウンロードして、HDD67に格納し(ステップS4)、ステップS3へ進む。

【0033】ステップS3で起動要求が与えられたと判断すると、ホスト用ドライバを起動する(ステップS5)。ホスト用ドライバを起動すると、セキュリティIDがSDカード13に設定済であるかを判断する(ステップS6)。具体的に、CPU41からSDカード13に対して、フラッシュROM111のログ情報格納領域111dにセキュリティID設定済か否かの問合せを行い、未設定であればSDカード13からID設定要求が、又設定済であればID設定済が返送されてくるので、この応答に基づいて判断する。ステップS6でセキ

ュリティID未設定の場合には、セキュリティID設定フェーズへ進み、セキュリティIDを設定する(ステップS7)。このセキュリティIDを設定することにより、ログ情報に対するアクセスに制限を加えることとなり、例えばSDカード13を紛失したり、盗難されたりして第三者の手に渡っても、不正にログ情報がダウンロードされることを防止することになる。

【0034】一方、ステップS6でセキュリティIDが設定済であると判断された場合、ホスト用ドライバは、セキュリティIDを追加設定するかの問合せ画面をLCDパネル7に表示させ、使用者に追加設定可否入力を促す(ステップS8)。ここでセキュリティID設定要の入力があれば(ステップS8)、セキュリティID設定フェーズへ進み、セキュリティID設定不要の入力があれば、ログ情報有無確認フェーズへ進んでログ情報の有無を確認する(ステップS10)。このステップS10では、SDカード13のログ情報格納領域111dから、セキュリティIDに対応したログ情報を取得し、無線通信リンク設定時の認証作業の簡略化を図る。

【0035】ステップS7又はS10の後、CPU41は、接続相手機器を特定した無線通信接続要求が与えられたかを判断する(ステップS11)。ステップS11でCPU41が接続要求が与えられたと判断すると、無線通信リンク設定フェーズへ進み無線通信リンクを設定する(ステップS12)。無線通信リンク設定フェーズでは、ステップS7において取得したログ情報、つまり過去に接続した相手機器情報がある場合、これを利用して認証作業を行う。無線通信リンクが設定された上で、対象データを所望の相手機器とSDカード13を介して無線通信する(ステップS13)。無線通信が終了する

と、MPU125は相手機器との無線通信に関するログ情報を作成し、ログ情報格納領域111dに格納する(ステップS14)。ログ情報格納時に、既に同一のB/Dアドレスのログ情報があれば、この記憶されたログ情報と新たに作成したログ情報とを置きかえる。また、もし容量的にログ情報格納領域111dに追加して記憶することが不可能な場合には、接合日時が最も古いものと新たに作成したログ情報とを置きかえるよう動作する。【0036】上述したセキュリティID設定フェーズ、ログ情報有無確認フェーズ、及び無線通信リンク設定フェーズについては、それぞれ図面を参照しつつさらに詳細に説明する。

【0037】セキュリティID設定フェーズは、図7乃至図9を用いて説明する。

【0038】セキュリティID設定フェーズが開始すると、CPU41はLCDパネル7にセキュリティID設定画面を表示する(ステップS100)。この設定画面は、例えば図8に示すように、8桁のセキュリティID入力領域と、「設定実行」「キャンセル」の入力用アイコンを含んでいる。上記セキュリティIDは8桁に限るのではなく、その長さは適宜選択、設定できるものである。ステップS100において、所定時間以内、例えば5分以内、にセキュリティIDの入力が与えられなかった場合はキャンセルアイコンがクリックされると、CPU41はSDホストコントローラ53に、SDカード13へ終了コマンドを送出させる(ステップS101、S102)。終了コマンドの送出手は具体的に述べると、SD/I/Oコントローラ113の入力データレジスタ113cに終了コマンドの情報が書き込むと共に、制御レジスタ113aの中の書き込みを示すビットの状態を変化(「0」→「1」)させることである。こうすることによってMPU125が、終了コマンド情報を受け取り、SDカード13の終了動作を行う(ステップS103)。以降SDホストコントローラ53がコマンドや情報をSDカード13に送出すると記載する場合は、上述のようにSD/I/Oコントローラ113の制御レジスタ113a及び入力データレジスタ113cにデータを書込むことを意味する。ステップS102、S103の後パソコン1及びSDカード13はそれぞれ図6の初期状態へ戻る。

【0039】ステップS101において、例えば図9に示すようにセキュリティIDがキーボード3から入力され、設定実行アイコンがクリックされると、CPU41は書き込みコマンドをSDホストコントローラ53からSDカード13へ送出させる(ステップS104)。書き込みコマンドを受領すると、SDカード13のMPU125は書き込み準備を行う(ステップS105)。ステップS103に続いてCPU41は、キーボード3から入力されたセキュリティIDを、SDホストコントローラ53からSDカード13へ送出させる(ステップS10

6)。SDカード13のMPU125は、このセキュリティIDを受領すると、フラッシュROM111のログ情報格納領域111dに格納する(ステップS107)。セキュリティIDの送出後、CPU41は、SDホストコントローラ53に対し、SDカード13へ終了コマンドを送出させる(ステップS108)。SDカード13のMPU125は、終了コマンドを受領すると終了動作を実行する(ステップS109)。ステップS108及びS109の後、パソコン1及びSDカード13はセキュリティID設定フェーズを終了する。

【0040】次に、ログ情報有無確認フェーズについて、図10乃至図14を参照して説明する。

【0041】ログ情報有無確認フェーズが開始すると、CPU41は、ホスト用ドライバに従い、LCDパネル7にセキュリティID入力画面表示を行う(ステップS200)。この入力画面は、例えば図11に示すように、8桁のセキュリティID入力領域と、「送信」「キャンセル」の人力用アイコンを含んでいる。ステップS200において、所定時間以内、例えば5分以内、にセキュリティIDの入力があされない又はキャンセルアイコンがクリックされると、CPU41は、SDホストコントローラ53に、SDカード13へ終了コマンドを送出させる(ステップS201、S202)。SDカード13のMPU125がここで終了コマンドを受領すると、終了動作を行い、ログ情報有無確認フェーズを終了する(ステップS203)。こうして終了した場合、以降のフローではログ情報が無いものとして処理されることになる。

【0042】ステップS201において、例えば図12に示すようにセキュリティIDがキーボード3から入力され、送信アイコンがクリックされると、CPU41は入力されたセキュリティIDの情報をSDホストコントローラ53からSDカード13へ送出させる(ステップS204)。セキュリティIDを受信すると、SDカード13のMPU125は、フラッシュROM111のログ情報格納領域111dに格納されたセキュリティIDと比較する(ステップS205)。比較の結果、ログ情報格納領域111d内に受信したセキュリティIDと一致するものがあるか否かは判断し(ステップS208)、一致するものがある場合には、アクセス許可情報をSD/IOコントローラ113の出力データレジスタ113bにセットし、出力データレジスタ113bにデータセットしたことを示す制御レジスタ113aの所定ビットを変更(「0」→「1」)する(ステップS207)。この状態にすることにより、SDホストコントローラ53が所定のタイミングで制御レジスタ113a及び出力データレジスタ113bにアクセスする際、SDカード13からデータを取得可能となる。このようにログ情報にアクセスできるようにすることにより、アクセス制限を解除する。SDカード13側のこのような動作

を、以降「情報を提示する」と記載する。

【0043】SDホストコントローラ53が、SD/IOコントローラ113にアクセスしてアクセス許可情報を取得すると、CPU41はアクセス許可状態であることをLCDパネル7に、図13に例示するような形態で表示する(ステップS208)。そしてCPU41は、SDホストコントローラ53を介して、SDカード13に対して、ログ情報読み要求コマンドを送出する(ステップS209)。読み要求コマンドを受領するMPU125は、ログ情報格納領域111dの対応するログ情報をSD/IOコントローラ113の出力データレジスタ113bにセットすることにより提示する(ステップS210)。SDホストコントローラ53は出力データレジスタ113bにアクセスし、ログ情報を読み主メモリ47へ転送することにより提示する(ステップS211)。このようにしてSDカード13からSDホストコントローラ53へ出力され、主メモリ47へ転送されるログ情報は、図14に示す情報から構成されている。

【0044】一方、ステップS206でログ情報格納領域111dに、SDホストコントローラ53から送られたセキュリティIDと一致するものがないと判断した場合、SDカード13は不一致情報を提示する(ステップS212)。SDホストコントローラ53が、SD/IOコントローラ113にアクセスして不一致情報取得すると、CPU41はセキュリティIDが不一致であり、ログ情報へのアクセスが拒否されたことをLCDパネル7に、図15に例示するような形態で表示する(ステップS213)。そしてCPU41は、セキュリティIDの不一致が3回連続であるかを判断する(ステップS214)。連続3回に達していない場合は、ステップS200へ戻り、再度セキュリティIDの入力を使す。しかし連続3回不一致であると判断された場合には、ステップS202へ進み、ログ情報無しとしてログ情報有無確認フェーズを終了することになる。

【0045】上述の通り、ログ情報有無確認フェーズでは、セキュリティIDが一致した場合に限りパソコン1側がSDカード13に記憶されたログ情報を取得することができるよう動作する。

【0046】最後に無線通信リンク設定フェーズの詳細について、図16乃至図19を参照して説明する。

【0047】パソコン1のCPU41は、まずSDホストコントローラ53に対し、SDカード13へ問合せ要求送信コマンドを送出する(ステップS300)。問合せ要求送信コマンドを受領すると、コントローラ12、つまりMPU125、リンクコントローラ129、及びRF部121と、アンテナ105を介しておよそ半径10m以内にある周囲の機器へ問合せ要求を送信する(ステップS301)。これは周囲の無線通信可能な機器を探索することである。Bluetooth方式で通信可能な外部機器がこの問合せ要求を受信すると、問合せ

せ応答を返信する(ステップS302、S303)。問合せ応答には、外部機器のデバイスアドレス(以下、B Dアドレスと称する)、端末種類、及び無線通信の同期をとるために必要な通信クロック情報が含まれている。SDカード13が、アンテナ105を介して問合せ応答を受信すると、MPU125は、受信情報つまり周囲の機器の探索結果を提示する(ステップS304)。このようにしてSDカード13から出力される周囲の機器の探索結果をSDホストコントローラ53が取得すると、主メモリ47にログ情報が有るか否かを判断する(ステップS305、S306)。SDカード13から出力されたログ情報が主メモリ47にある場合には、受信情報のBDアドレスと一致する機器、ログ情報にのみ存在する機器、及び受信情報にのみ存在する機器をそれぞれ区別して表示する(ステップS307)。CPU41はLCDパネル7に、例えば図17に示すようにログ情報及び受信情報を表示する。受信情報のBDアドレスと一致する機器は、プリンタD1のようにログ情報と共に通常表示とすることにより受信情報に含まれて現在接続可能であることを表示する。このように表示された機器は無線通信リンク設定時の認証作業を短縮できる機器であることを意味する。ログ情報にのみ存在し受信情報にない機器は、FAXD2のように反転表示とした上でログ情報を表示する。このように表示することにより受信情報にないこと、つまり問合せ時点で周囲に通信可能として存在していないことを示す(図外を示す)。受信情報にのみ存在する機器は、パソコンD3のように通常表示として現在接続可能を示すもののログ情報表示していないため、過去に接続したことがない機器であることを示す。このように、無線通信リンク設定時の認証作業を短縮できる機器とできない機器、さらに短縮可だが接続できない機器とを区別させることができる。

【0048】ステップS306において、主メモリ47にログ情報が無いと判断された場合は、受信情報のみを表示する(ステップS308)。

【0049】ステップS307、又はS308にてLCDパネル7に表示された機器のいずれかがキーボード3により選択されると(ステップS309)、CPU41は、その選択入力された機器AのBDアドレス(例えばプリンタD1の「10-00-22-33-44-55」を用いて、SDホストコントローラ53からSDカード13へ呼出し送信コマンドを送出させる(ステップS310)。SDカード13では、コントローラ101からアンテナ105を介して上記特定のBDアドレスを用いて機器Aへ呼出しを送信する(ステップS311)。このBDアドレスの機器Aは、呼出しを受信すると、自分のBDアドレスを含む呼出し応答を送信する(ステップS312、S313)。SDカード13では、この呼出し応答を受信すると、コントローラ101は、自機の情報を機器Aへ無線送信する(ステップS3

14、S315)。この自機の情報には、SDカード13のコントローラ101を含む無線通信部にBDアドレス、端末種類、及びクロック情報を含んでいる。機器Aは、SDカード13からの情報を受信すると、データを記憶して、受信したことを示す受信通知を無線送信する(ステップS316、S317)。SDカード13が受信通知を受信すると、Link Keyの有無、つまりログ情報の有無に応じて、異なるステップへ進む(ステップS318、S319)。Link Keyがある場合には、図18のAuthenticationステップへ進み、Link Keyが無い場合には、図19のPairingステップからLink Key生成ステップへ進む。因みにLink Keyとは128ビットの秘密鍵であり、接続防止と盗聴防止の管理のために使用される。このLink Keyは無線通信リンクを確立に伴い生成される。

【0050】図18では、まずAuthenticationステップの中で、SDカード13内で乱数Aを発生し、外部の機器Aに送信する(ステップS320)。その後SDカード13と機器Aとで並行して認証用データの作成を行う(ステップS321、S322)。認証用データの作成には、SDカード13と機器Aとがそれぞれ記憶している同一のLink Key、乱数A、機器AのBDアドレスとを用いられ、且つ同一の演算により求められる。従って、そこから得られる認証用データは通信異常が無い限り一致するはずである。

【0051】ステップS322において認証用データ作成の後、機器Aは作成した認証用データを無線送信する(ステップS323)。SDカード13は認証用データを受信すると、自ら生成した認証用データと比較し、一致しているか否かを判断する(ステップS324、S325)。比較の結果不一致であれば、機器Aに対し不一致を通知し、さらにパソコン1に対して認証失敗を提示する(ステップS326、S327)。SDカード13はこの状態でステップS311の呼出し送信の前の状態となる。不一致を受信した機器Aは、ステップS312の呼出し受信の前の状態へ戻る(ステップS328)。SDホストコントローラ53は、認証失敗の情報を取得すると、CPU41がこれをLCDパネル7に表示し、ステップS315へ戻る(ステップS329)。

【0052】ステップS325において、認証用データが一致していると判断した場合、SDカード13は機器Aに対して認証データの一致を通知する(ステップS330)。このステップS330までがAuthenticationステップであり、次にSDカード13と機器Aとの間で暗号化キー生成すると(ステップS331)、無線リンクが確立する。SDカード13のMPU125は、無線リンク確立したことを提示し、SDホストコントローラ53がこの情報を取得すると、CPU41はLCDパネル7に無線リンク確立したことを表示す

る(ステップS332、S333)。こうしてログ情報がある場合の無線通信リンク設定フェーズを終了する。

【0053】これに対しステップS319において、Link Keyが無い、つまりログ情報が無いと判断された場合の無線リンク設定フェーズの後段部分について図19を用いて説明する。

【0054】まずPairingステップの中で、SDカード13内で乱数Cを発生し、外部の機器Aに送信する(ステップS350)。機器Aは乱数Cを受信するとSDカード13へ受信確認を送信し、図示しない表示部にPINコード入力要求を表示する(ステップS351、S352)。PINコードとは、使用者が任意に設定することのできる8ビットのコードである、Link Keyを持たない機器同士で無線通信リンクを確立する場合、誤接続を防止や盗聴防止のために、それぞれの機器から同一のPINコード入力を行うようになっている。

【0055】ステップS352の表示の後、特定のPINコードが入力されると、このPINコード、乱数C、及び自機(機器A)のBDアドレスから仮のLink Keyを生成する(ステップS353、S354)。

【0056】ステップS351にて機器Aが送信した受信確認をSDカード13がアンテナ105を介して受信すると、MPU125はPINコード入力要求情報を提示する(ステップS355)。SDホストコントローラ53がSD/IOコントローラ113からPINコード入力要求情報を取得すると、CPU41は、LCDパネル7にPINコード要求画面を表示する(ステップS356)。キーボード3によりPINコードが入力されると、CPU41はこのPINコード、乱数DをSDホストコントローラ53を介してSDカード13へ送出する(ステップS357、S358)。ここで入力されるPINコードは、ステップS353にて機器A側で入力有を判断したPINコードと同一でなければ、無線通信リンクは確立できない。

【0057】SDカード13のMPU125は、受領したPINコード、乱数C、及び相手機器AのBDアドレスから仮のLink Keyを生成する(ステップS359)。続いてSDカード13は、乱数Dを生成して機器Aへ送信し、さらにこの乱数D、ステップS359で生成した仮Link Key、及び機器AのBDアドレスから認証用データを生成する(ステップS360、S361)。

【0058】SDカード13から乱数Bを受信すると、機器AでもSDカード13と並行してステップS361と同様に認証用データの作成を行う(ステップS362)。ステップS361及びS362での認証用データ作成は、SDカード13と機器Aとがそれぞれ記憶している、PINコードが同一であれば同一であるはずの仮Link Key、乱数B、及び機器AのBDアドレス

が用いられ、所定の演算により求められる。つまりここでは同じ変数を用いて同じ演算を行うので、そこから得られる認証用データは一致するはずである。

【0059】ステップS362において認証用データ作成の後、機器Aは作成した認証用データを無線送信する(ステップS363)。SDカード13は認証用データを受信すると、自ら生成した認証用データと比較し、一致しているかを判断する(ステップS364、S365)。比較の結果不一致であれば、機器Aに対し不一致を通知し、さらにパソコン1に対して認証失敗を提示する(ステップS366、S367)。SDカード13はこの状態でステップS311の呼出し送信の前の状態となる。不一致を受信した機器Aは、ステップS312の呼出し受信の前の状態へ戻る(ステップS368)。SDホストコントローラ53は、認証失敗の情報を取得すると、CPU41がこれをLCDパネル7に表示し、ステップS315へ戻る(ステップS369)。

【0060】ステップS365で認証用データの一致を判断すると、SDカード13は、機器Aへ一致を通知する(ステップS370)。このPairingステップは、このステップS370で終了し、次にLink Key生成ステップへ進む。ステップS370の後、SDカード13は乱数Eを発生し、この発生した乱数E、自機(機器A)のBDアドレス、及び仮Link KeyからLink Key(A)を生成する(ステップS371、S372)。

【0061】一方SDカード13から認証用データの一一致の通知を受けると、機器A側でも独立して乱数Fを発生し、この乱数F、自機(機器A)のBDアドレス、及び仮Link KeyからLink Key(B)を生成する(ステップS373、S374)。Link Key(A)及びLink Key(B)は、それぞれ異なる乱数及びBDアドレスにより求められるため、一致することは無い。SDカード13と機器Aとは、互いにLink Key(A)及び(B)を相手に送信して共有した後、予め決められたルールに従いLink Key(A)及び(B)のいずれをLink Keyとするかを決定する(ステップS375、S376、S377)。

【0062】このステップS377までがLink Key生成ステップであり、次にSDカード13と機器Aとの間で暗号化キーを生成すると(ステップS378)、無線リンクが確立する。SDカード13のMPU125は、無線リンク確立したことを提示し、SDホストコントローラ53がこの情報を取得すると、CPU41はLCDパネル7に無線リンク確立したことを表示する(ステップS379、S380)。こうしてログ情報が無い場合の無線通信リンク設定フェーズを終了する。

【0063】図18では、図19における認証作業の中でPINコード入力に伴う部分がなく、またLink Key生成ステップに相当する箇所も無い。このように

図18は図19に比較して明らかに短縮化した流れとなっている。

【0064】上記パソコン1からSDカード13を取り外し、PDA21に装着して無線通信にしようする場合、ログ情報の活用を含め制御の流れは上記説明と同様である。つまり、パソコン1のキーボード3をPDA21の入力ペン25とタッチセンサパネル93へ、LCDパネル7をLCD91へ、CPU41をCPU81へ、主メモリ47をRAM87へ、SDホストコントローラ53をSDホストコントローラ95、HDD67をフラッシュROM85へ、PCバス81を内部バス83へ、それぞれ置き換えると、図6乃至図19において説明した内容と同じ流れとなる。

【0065】以上詳述した通り、SDカード13のフラッシュROM111内にログ情報格納領域111dを設け、このSDカード13がパソコン1等ホスト装置に装着されて外部機器と無線通信を行った際のログ情報をこのログ情報格納領域111dに保存する。次にPDA21等のホスト装置から上記同一の外部機器と無線通信する際に上記ログ情報格納領域111dからログ情報をダウンロードして利用する。従って、ホスト装置が変わってもSDカード13と接続先の外部機器とが同一であれば、無線リンク確立を簡略化することができる。

【0066】なお、この発明は上述した実施の形態に限定されることなく、この発明の主旨を逸脱しない範囲で種々変形可能である。例えば、通信装置はSDカードでなくPCカードであっても構わない。この場合PCカードに不揮発性メモリを設け、その中にログ情報格納領域を設定すれば、上記SDカードの場合と同様にPCカードスロットを有するホスト装置間で装着変更に関わらず、無線リンク確立の簡略化を図ることが出来る。

【0067】また複数のセキュリティIDでなく、単一のセキュリティIDのみを設定するようにしてもよい。

【0068】無線通信方式は、Bluetooth方式に限らず、無線リンク設定時にログ情報、特に鍵情報の有無によって異なる手順で動作するものであれば構わない。

【0069】

【発明の効果】以上詳述したように、本発明によれば、過去に接続したことのある外部機器と接続する場合には、通信装置が装着されるホスト装置が異なっても無線通信リンク確立作業を簡略化することができる。

【0070】さらに、通信履歴情報に対するアクセスに制限を加えることができるので、通信装置の紛失や盗難により第三者に渡ってしまったとしても、通信履歴情報を不正にダウンロードされることを防止できる。

【図面の簡単な説明】

【図1】この発明の実施の形態に係る無線通信ネットワークを示す図。

【図2】同実施形態におけるパーソナルコンピュータの

構成を示すブロック図。

【図3】同実施形態におけるPDAの構成を示すブロック図。

【図4】同実施形態のSDカードの流れを示す図。

【図5】本実施形態のフラッシュROM内のデータ構造を示す図。

【図6】本実施形態の無線通信動作の全体の流れを示す図。

【図7】無線通信動作のセキュリティID設定フェーズの流れを示す図。

【図8】セキュリティID設定フェーズにおけるセキュリティID設定画面を示す図。

【図9】セキュリティID設定画面でセキュリティIDを入力した状態を示す図。

【図10】無線通信動作のログ情報確認フェーズの流れを示す図。

【図11】ログ情報確認フェーズにおけるセキュリティID入力画面を示す図。

【図12】セキュリティID入力画面でセキュリティIDを入力した状態を示す図。

【図13】セキュリティID入力後のログ情報に対するアクセス許可の表示例を示す図。

【図14】ログ情報確認フェーズでSDカードから出力されるログ情報表示例を示す図。

【図15】セキュリティID入力後のログ情報に対するアクセス拒否の表示例を示す図。

【図16】無線通信動作の無線通信リンク設定フェーズの流れを示す図。

【図17】無線通信リンク設定フェーズにおけるログ情報と受信情報の表示例を示す図。

【図18】無線通信動作の無線通信リンク設定フェーズの簡略化した無線リンク確立手順の流れを示す図。

【図19】無線通信動作の無線通信リンク設定フェーズの簡略化しない無線リンク確立手順の流れを示す図。

【符号の説明】

1…パーソナルコンピュータ

3…キーボード

7…LCDパネル

13…SDカード

15…SDカードスロット

21…PDA

27…SDカードスロット

41…CPU

47…主メモリ

53…SDホストコントローラ

105…アンテナ

111…フラッシュROM

111d…ログ情報格納領域

113…SD/IOコントローラ

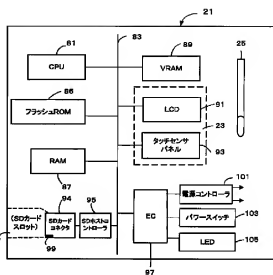
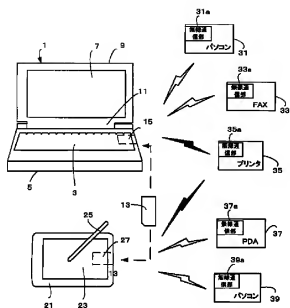
121…RF部

123…ベースバンドコントローラ

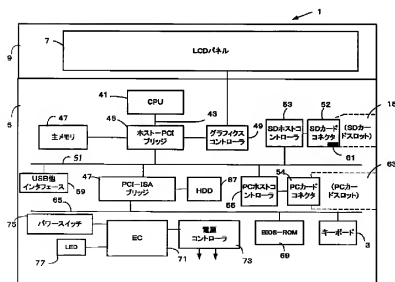
* * 125…MPU

【図1】

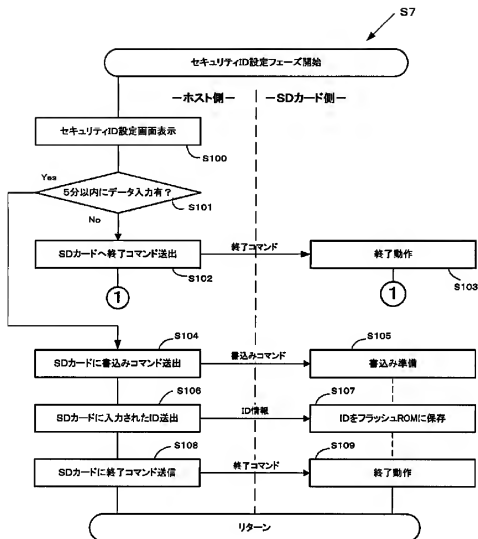
【図3】



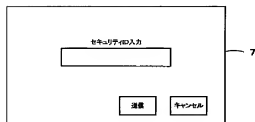
【図2】



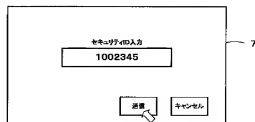
【図7】



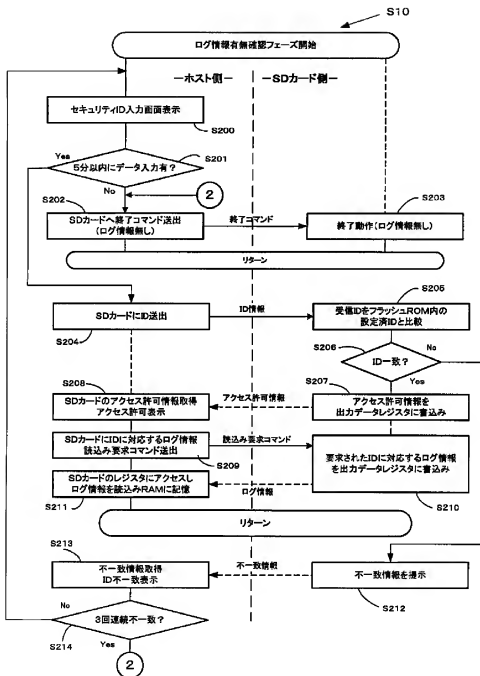
【図11】



【図12】



【図10】



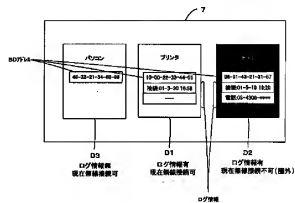
【図13】

【図14】

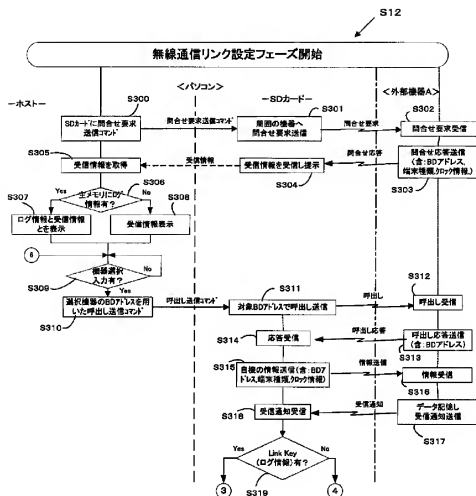
セキュリティID	1002345
機器名称	プリンタ
BDアドレス	10-00-22-33-44-55
接続時間	01:23:40
接続日時	2001-03-20 16:58
電話番号	---
Link Key	012345abcd

【図15】

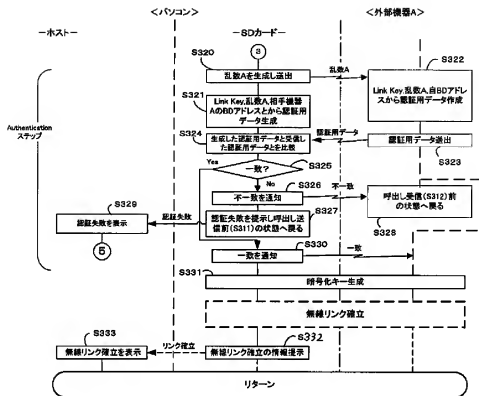
【図17】



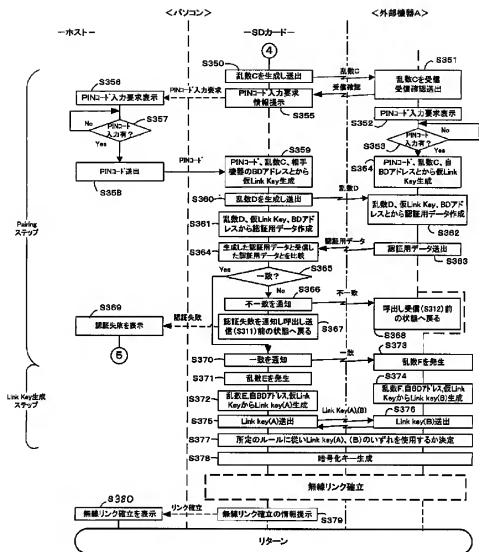
【図16】



【図18】



【図19】



フロントページの続き

F ターム (参考) 5C062 AA02 AA14 AA27 AA37 AB38
 AB42 AC22 AC34 AC58 AF00
 BD09
 SK033 AA08 AA09 DA19 DB12 DB14
 SK034 AA19 DD02 EE03 KK21
 SK067 AA21 BB02 EE02 EE10 EE16
 GG06 HH12 HH12 HH24